LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

GDPR readiness assessment for healthcare company

Lähdemaa, Niko

Laurea University of Applied Sciences

GDPR readiness assessment for healthcare company

Niko Lähdemaa
Security Management
Bachelor's Thesis
May, 2017

Laurea University of Applied Sciences
Degree Programme in Leppävaara
Bachelor's Thesis

Abstract

Niko Lähdemaa

GDPR readiness assessment for healthcare company

Year 2017 Pages 38

The purpose of this thesis is to evaluate the current state of information security for a company which is providing healthcare services. The target is to map their GDPR readiness, raise the understanding of information security, enhances existing processes and improves inner communication inside of organisation. The company was registered in the trade register in 2011 as a joint-stock company. The business industry of the company is other healthcare services (86909), which mean they have to take information security into account in business decisions. The company gather sensitive information from their customers to do their business. Project scope cover the methods of how the company storage sensitive data, the durability and destruction of tools at the end of the equipment life cycle. The research project itself include sensitive information about the case company's processes, so together with the company's CEO (Chief executive officer) we decided not to publish their name on draft versions or on final project report. Research project is done by interviewing the main stakeholder of the company. The questions are chosen from the ISO 27001 security frameworks. I have selected the main divisions of the above mentioned standards to meet small- or medium sized enterprise security needs. During the project the data breaches, development suggestions and target states are reviewed with the company's CEO. The final report will be handled to CEO in summer 2017 and the acute development proposals will be evaluated in inner meetings. It is important to remember that the company is still small sized enterprise and therefore the development must be made according to the company's financial capabilities. The company has been interested to find out about the privacy regulations that apply to them in 2018. GDPR comes in to effect in 2018, so this mean every company who is doing their business in European Union area or handles information considering the citizens of EU has one years left to meet compliance requirements of GDPR (General Data Protection Regulation). The security regulations are generally seen as limiting factor to companies' business. Their implementation into a working process seems to be hard and expensive, which is usually not the whole story in the long run. After the final project meeting, the aim is to get the company's main stakeholders to understand with the security management they can observe their critical controls, constantly develop the level of security and expand their future business more effectively.

Keywords: Information security, GDPR, Data protection

Laurea University of Applied Sciences **Tiivistelmä**
Degree Programme in Leppävaara
Bachelor's Thesis

Niko Lähdemaa

GDPR readiness assessment for healthcare company

Vuosi 2017 Sivumäärä 38

Tämän lopputyön tarkoituksena on kartoittaa Helsinkiläisen terveyspalveluita tarjoavan yrityksen tietoturvallisuuden nykytila ja nostattaa tietoturvan ymmärrystä, tehostaa olemassa olevia prosesseja ja parantaa kommunikaatiota yrityksen sisällä. Tarkoituksena on vertailla heidän nykytilaa GDPR:n tuomiin lisävaatimuksiin. Yritys on rekisteröity kaupparekisteriin vuonna 2011 osakeyhtiönä. Toimialana yrityksellä on muut terveyspalvelut (86909) mikä tarkoittaa, että yrityksen on otettava huomioon yritykseen liittyvissä liiketoimintapäätöksissä tietoturvallisuus tarkasti. Yritys kerään luottamuksellista tietoa asiakkaistaan terveyspalveluita varten, joten tarkastuksen kohteena ovat myös sensitiivisen tiedon säilytystapa, työvälineiden riittävyys ja tuhoaminen laitteiden elinkaaren päätyttyä. Lopputyön luonteen takia olemme päättäneet yrityksen toimitusjohtajan kanssa tehdä selvitystyön ilman, että mainitsemme heidän nimeä lopullisessa raportissa. Selvitystyö tehdään haastattelujen perusteella käyttäen laatimaani kysymysrunkoa joka perustuu ISO 27001 tietoturvastandardiin. Olen valinnut keskeiset jaostot edellä mainitusta standardista, jotka vastaavat pien-keskisuuren yrityksen tietoturvatarpeita. Työn aikana esille nousseet tietoturvapoikkeamat, kehitysehdotukset ja tavoitetila käydään läpi yrityksen johtoryhmän kanssa keväällä 2017 ja akuutit kehitysehdotukset käydään läpi niin sanotuissa väliaikatapaamisissa. On tärkeä muistaa, että yritys on vielä kooltaan Pk-yritys ja sen takia kehitysehdotukset on solmittava yrityksen taloudellisen kyvykkyyden mukaan. Yritys on ollut erityisen halukas saada selvityksen heitä koskevista tietosuoja-asetuksista, jotka astuvat voimaan keväällä 2018. Tämä tarkoittaa, että kaikilla yrityksillä jotka toimivat Euroopan Unionin alueella tai käsittelevät tietoja Euroopan Unionin asukkaista on kaksi vuotta aikaan implementoida tietosuojakäytännöt osaksi heidän liiketoimintaansa. Vertaan havaintoja joita teen projektin aikana uuteen Euroopan Unionin tietosuoja lainsäädäntöön (General Data Protection Regulation). Turvallisuusasetukset koetaan yleensä yrityksissä rajoittavina tekijöinä ja niiden implementointi voi tuntua kalliilta ja raskaalta mikä ei kumminkaan yleensä pidä paikkaansa pitkässä juoksussa. Lopullisen projektikokouksen jälkeen tarkoitus on saada yrityksen johtoryhmä ymmärtämään, että turvallisuus yrityksessä tuo liiketoiminta varmuutta ja oikein tehtynä se helpottaa jo olemassa olevien, kuin tulevien prosessien käyttöönottoa.

Avainsanat: Tietoturva, GDPR, Tietosuoja

Table of Contents

1 Introduction

This thesis is done for a small sized healthcare organisation. The company was registered in the Finland's trade register in 2011 as a joint-stock company. The business industry of the company is other healthcare services (86909), which mean they have to take information security into account in their business decisions. The project scope was to define their current readiness for upcoming information security and data protection regulation. The main target is to map their GDPR readiness, raise the understanding of information security amongst the main stake holders, enhances existing processes and improves inner communication inside of the organisation. All the organisations whose business is done in European Union member states or they are handling information considering EU citizens despite of the business industry have to evaluate their information security readiness and possible security gaps which have to be mitigated before 25th of May. This is to date when the new general data protection regulation comes into effect in all European Union member states.

After this security assessment the company is more likely to understand their current strengths and weaknesses. In the same way they get information how to avoid unnecessary risks to happen and what are the ways of building stronger business security culture. The good security inside of organisation is not a thing which is made once and it last forever, so the companies needs to continually adjust security processes to meet requirements of todays' world and increase the knowledge how to mitigate unwanted risks and threats to happen. Understanding the current state is essential to do especially when the company tries to achieve their business goals, get better turnover from their business investments, expand their business and protect business continuity. These are essential parts of building a good readiness assessment for GDPR requirements (Figure 3).

The upcoming regulation is the largest reform of global privacy and data protection laws in 20 years. This doesn't mean that everything is going to change. The new regulation can be seen as an updated version of many existing directives which brings together and update all the essential privacy parts from each directive (European council). The companies' still have one year left to implement new processes into their business, but now it's time to act and take the first steps. The first project phases included the interviews with the CEO where we decided how the project will be accomplished and who will be the key personnel whose take part of this project. The GDPR is the main driver for the project, but I'll also try to find critical risks which may have influence on company's business.

Finally, I will present all of my recommendation to company's main stakeholder. Together with the main stakeholder the accepted recommendation are implement into their risk policy. Together we'll implement the updated policies into companies' processes and choose cost

effective solutions to maintain the necessary security level. I'll try to emphasize the well-structured polices work as a guidelines and ways of working instead of restrictive regulations. With these policies I'll try to help the growing business observe their critical controls, constantly develop the level of security and expand their business more effectively. It is important the owners of the company understand the regulation, so we can build consensus and start developing company's processes (Figure 3).

2 Cyber security trends

Limnéll (2014) made a statement the awareness of information security has increased over the last years amongst the users. Between these years we have noticed the information security with developing technology is basic need for all of us and we couldn't cope without the technological solutions anymore.

This statement is pretty obvious because, if you stop for a while and start thinking the services what you have used during the week. You quickly recognize we all use and enjoy the services which are results of technology developments. The technology and web-based services has a significant part on our everyday life and through the internet and web based applications we control even the most critical infrastructure to the society. This why, even the smallest failures or security breaches to the critical processes can have a massive impact on us. The developing technology brings us new effective opportunities but the new opportunity brings us the new risks to control.

In a smaller scale we can think the main stakeholders of the companies might have similar kind of problems to face. Their customers and employees strongly rely that everything is working and their sensitive personal data is protected in all causes. This brings major responsibilities for different organisations and this why many of the companies have needed to adjust their security policies to comply with legal and security regulation requirements of today. Many companies can save resources and money only of understanding their business related critical risks and current risk appetite. This how to resources are targeted on essential processes and taken away from unnecessary processes which not directly threaten the organisation's business.

We all know the world is developing fast and it's easy to find technological solutions to prevent mistakes to happen, but many information security experts like Krazit (2016) has emphasized we have to get rid of this ideology that everything can be fixed with buying new technological services. It's the best take few steps backward and think the basic factors which might cause the errors and understand even the most developed technological solutions are run by employees. Ponemon institute with IBM made large global research project last year consider-

ing the data breaches. The study included information from 383 enterprises from twelve different countries (Figure 1).

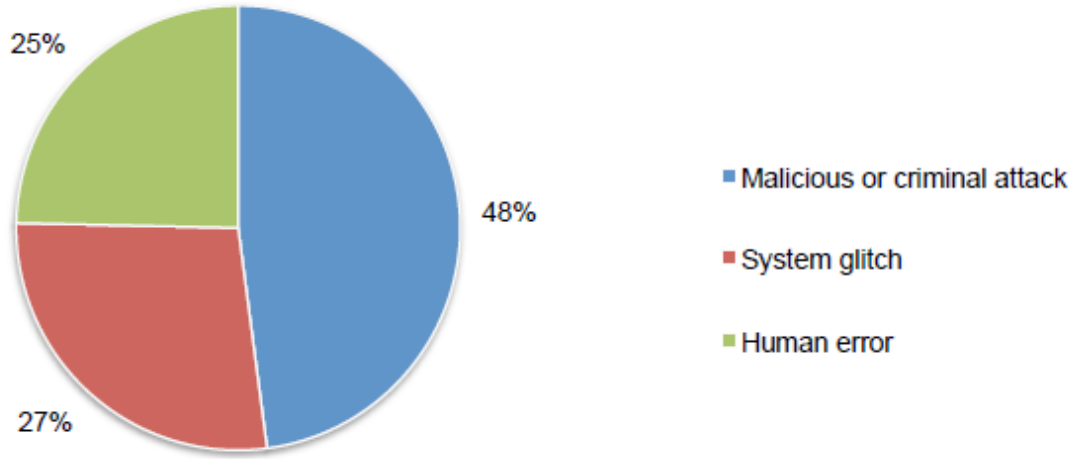


Figure 1 Cause of the data breach

The study back-up Krazit's (2016) statement the human is usually the companies' weakest link when we speak about information security. This thesis tries to emphasize it's all the employees' responsibility to do their everyday work with taking security into account. But it's employers' responsibility to set boundaries, provide the right tools and instructions to its employees. The more sophisticated technological solutions can prevent or slow down the attackers, but this small organisation doesn't have resources to invest in expensive systems, so it's better to focus on preventing human errors.

3 Risk management

Limnéll (2014) emphasized the security needs to be seen as a positive thing for companies. We can read almost every day from media about new data breaches and criminal acts which have been made through the internet. Still the "age of digitisation" and new web based innovations give us more positive than negative things. The web based services have changed how we are doing everyday common tasks and work related tasks more effectively. This why the information security should be seen as an essential tool to ensure the functioning of web based services. Too often the companies seem to think the security is only a cut for possible business profits. But the whole security ideology should be seen as supporting act to achieve business goals and avoid relevant risks to help the company.

The world is full of regulations and instructions how the companies can increase their information security capabilities and mitigate the unwanted risks to happen. Chambers (2015) the former chief execution officer of Cisco Company has said “In this world there are two types of companies. Those companies that have been hacked and those ones who don’t know they have been hacked”. This why it’s the best take cyber security threats seriously and try to prevent any major mistakes to happen or at least those situations that would have been preventable with proper security management.

The situational crime prevention culture inside of the organisation can be done by offering fewer opportunities for attackers (Clarke 1997). For example by understanding the basic principles of social engineering can prevent human error breaches. The hardened targets like educated people, encrypted systems and safe networks attract fewer attackers (Anatomy of a data breach). You can’t protect yourself from all the threats, but it’s wise not to be the easiest target for the black hats. Gil (2017) described the black hats are usually computer users who has unethical purposes to cause chaos among normal computer users. The styles, reasons and methods vary, but one of most typical attack type against companies’ is DDoS (Distributed Denial of Service) attacks. In this method the attacker builds so much traffic and pressure on a website that it will shut down. These kind of attacks usually effect on company’s business continuity.

Of course these are the extreme examples and usually the most significant issues inside of the organizations are results of thinking the information security is only a technological matter. This is especially a problem in Finland where many companies doesn’t have any kind of coherent security culture. The security related tasks are thought to be only problems of one certain department or service provider. The security is not seen as a process where all the departments and employees have to work together to prevent mistakes to happen (Limnéll 2014).

From the Sans Institute IT top spending report 2016 we can draw a conclusion the companies are making preparations regarding the upcoming regulations. To protection of sensitive data is now the biggest investment area in IT-security (Figure 2)

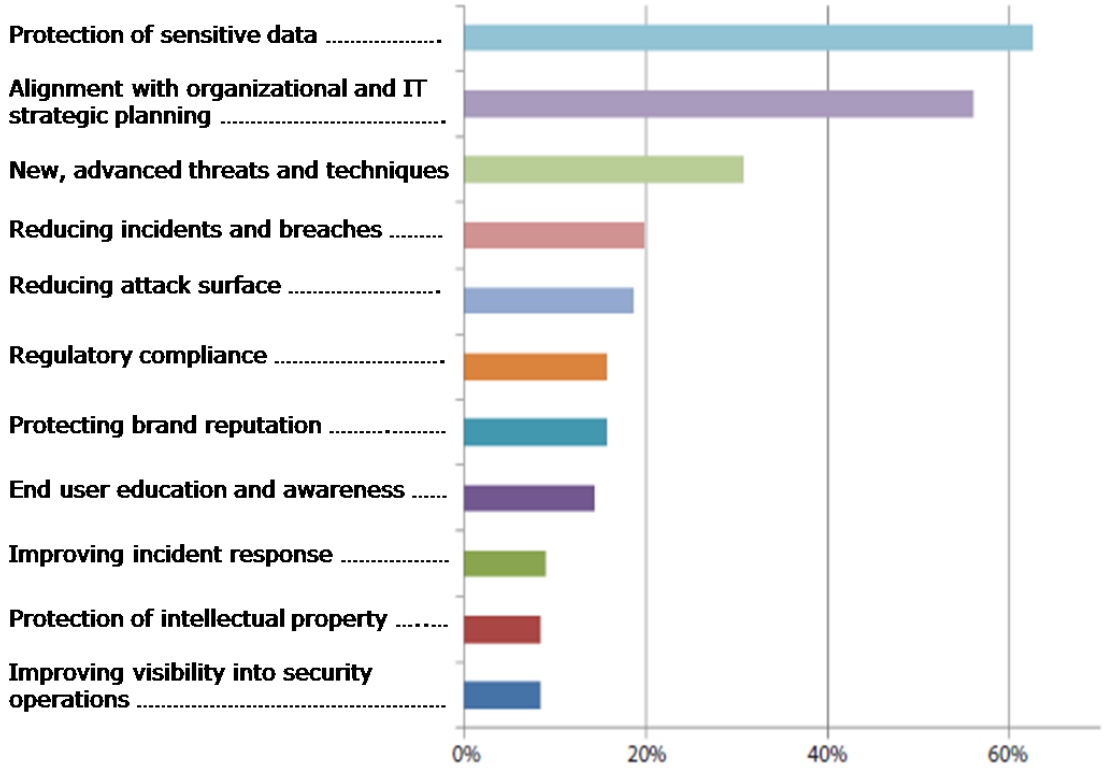


Figure 2 IT Security spending trends

IT security usually provides technological solutions and tools to prevent breaches (Filkins 2016), but policies can be seen as a rule book which enhances the overall security culture inside of the organisation. This readiness and current state assessment has been done for a small sized organisation and these companies usually have limited amount of resources to use for security, so the recommendation have to be in the same level with organisation's resource capabilities.

The current state assessment including the risk assessment is a comprehensive description and analysis of the risks or threats that can cause interruptions to business operations or otherwise complicate the continuity of business (Schmittling 2010). The business continuity management is designed to raise understanding towards positive and negative nature risks what company can face. The economic losses may be great for a small business in the operational interruptions, so the risk mapping provides information on their own critical information. The small and medium sized enterprise resources are limited usually towards security, so the resource allocation is important to target on critical business risks and reduce resources from the uncritical risks (Everest 2008).

Limnéll (2014) pointed out still in 2017 many companies doesn't have well-structured processes to control their risks and the policies are more than just rules on a paper for company employees'. The information security policy gives the clear processes and methods how to control the risks. The risks what an organisation face can be divided in three different sections. The risks what company sees as positive risks which might have an impact of growing business profit. Then the risks what are mandatory to take for operating the business. Especially these risks have to be evaluated and mitigated to meet companies' risk appetite. And finally the risks what company doesn't want to take and they have might have a negative impact for the business. In this thesis I will try to find critical unwanted risks and find cost effective solutions. The reasons for mitigating these unwanted risks are described in following chapters.

4 Case company

The project scope was chosen together with company's CEO. He asked me to help them to evaluate what is their current situation and what are the possible development areas they need to change before March 2018. The purpose of this project is to define how the information security policies and standards have been implemented into organisation processes. I have taken into account the main stake holders' existing information security knowledge and size of the organisation before doing the assessment. The case company asked me to give them an audit related project where the best practices are compared to their daily work. The research project itself include sensitive information about the case company's processes, so together with the company's CEO (Chief executive officer) we decided not to publish their name in draft versions or final project report.

The case company in this thesis project is a small healthcare service provider. There are specific obligations in GDPR that are addressed for the healthcare business industry and the most of them are listed as higher protection requirements. The company's core business is built around of helping the customers with their physical health issues. But only a few of these high standard requirements are directly linked to the case company and their business. The most important obligation is the data which is related to individual person's physical health should not be directly linked to person's personal information (Baiati 2017). This why I have recommend the company consider a service provider who can provide them a platform where the data can be divided into divisions. A platform where the admin can allow editing and access rights for only those employees who need them. The other recommendations for the company are presented in chapter 6.

The company is registered in the Finland's trade register in 2011 and since then they have doubled their profit revenue every year. At this moment the company has 24 employees and four main stakeholders. They have prospered in their business industry significantly well and they have made investments and expanding processes for upcoming years. At this moment the new clinics are mainly opened in Helsinki region but in the near future they are expanding their business in Finland's other major cities. The company hires new employees because of the expanding processes and therefore they will have more people for controlling the data considering their customers health in different locations. This is one of the main things what they need to think. The system and method has to be mutual for every employee, despite of their current location.

5 General Data Protection Regulation requirements

In 2017 many of the companies need to evaluate what is their current state when we speak about information security and data privacy. The negations within new data privacy regulation in European Union last more than four years. The European institutions, (EU Council, European Parliament and European Commission) agreed on a new Privacy Regulation on 15th December 2015. In this date they finalized the agreement for the upcoming data privacy regulation General Data Protection Regulation (GDPR). The application date for the regulation is 25th of May in 2018, so globally the companies have one year to adjust their privacy and data protection methods to meet the requirements of the General Data Privacy Regulation. Basically the content of GDPR is not new because the European Union already adopted data protection directive 95/46 in year 1995. The current directive includes many of the same sections than GDPR does (Church 2016).

The new data security regulation brings new general terms despite of the size of organisation, so the upcoming standard forces all the companies despite of their size to follow regulation. In basic principle the company can't explain their possible data breach by saying they are micro or small sized company. Of course the requirements for the case company are not in a same scale than they are for example the largest multinational organisations. And some of the individual requirements are only for organisations' which have more than 250 employees like appointing DPO (Data Protection Officer). But only the size of the company is not the right reason to neglect regulations (Boardman. 2017).

Figure 3 GDPR process implementation

The data protection and privacy has becoming important part of the everyday businesses inside of different sized companies. The law regulations and possible sanctions given by European Union inspector are the main drivers for many organisations to follow upcoming regulations. The sanctions vary from issue warnings to massive fines. The sanctions of severe violation or negligence to follow regulation can be up to companies' 4% of annual worldwide turnover or 20 million Euros. The random inspections by supervisory authorities can be done after May 2018 in any of the companies. At first the observation inspections works as to share information of GDPR, but later on they'll change more like audits (Church 2016).

6 Information security

The information security and data protection is often seen as a same thing. Data protection is intended to take the data subject into account, so the rights of individual people and the sections defined by the European Union and country specific laws are followed. The information security should be seen more like a tool how you can protect the data subject of individual person. It is more like operational security where different methods are implemented into company's practices. These operational security examples can be security monitoring, safe disposal of hardware, software update management, breach detection and different crime prevention methods (Opi tietosuojaa).

In this chapter I will also introduce my findings and the recommendations. The findings are categorized in three different chapters. The categories have been selected to meet the small and medium sized enterprise requirements. The guidelines for this current state assessment have been chosen from ISO 27001 frameworks. I will plan the engagement using a risk-based approach, where I emphasize my findings. I will identify the actions the company should take to improve compliance with the forthcoming regulation.

The findings and recommendations have been evaluated according to the following classification model. The tables can be found after the each chapter (Table 1).

High Risk The essential internal controls do not exist or they are not functional. The necessary controls must immediately determine or fix the existing controls.	**1**
Medium Risk The essential internal controls are partly existing and working. The corrective measures need to be defined and fixed on priority basis	**2**
Low Risk The significant internal controls are existing and functional, but the effectiveness of the controls can be improved.	**3**

Table 1 the risk level of findings

6.1 Information classification

The level of information classification is depending how important the data is for the company and what would happen if it would be leaked. The company itself needs to define the levels of information, how it is protected and who has the access to see the information. In the same way the company gets better understanding of their critical business context and objectives in order to enhance value from information security investments. Also for defining critical information the company understand their threat landscape and how to focus on the right prioritizes (Rodgers 2012).

The company should monitor the classification practices are followed for the physical and electronic material. The employees who are handling the sensitive information must have a clear guidance for permitted ways of handling classified material. The company has not clearly defined classification practices which apply to both electronic and physical data. This might result into situation where employees do the decisions where to storage classification data and how to share them amongst other employees. This is classical example of shadow it where the company's owners doesn't recognize all the needs and tools what employees needs to take care of their daily work. For example the employees might use outsourced free cloud services to storage work related materials whose security is not evaluated by company's own risk analysis (Rodgers 2012).

The company itself does not own the premises or other major assets, so it is clear most critical assets for the company are their customers, so this why the customer data has to be protected. All the information (both oral and written) which is linked company's current and past customers should be classified as confidential information. The security of this confidential information is essential to handle with good care and limit the access rights only for those who need to see information. The publicized privacy breach may result to damaged reputation and it might have serious consequences to this size of organisation. The information security policy should include at least following things.

After the data or information has been created or collected the correct ways of storing it has to be defined. For example the case company should make two different places to store personal information. The one only for customer data where is restricted access only for those who needs the data. The second place to save the employees data e.g. bank account numbers, working hours etc.

It’s not easy to protect information for its whole lifecycle, so that’s why it is important to follow the policies and rules. All the security policies and guidance should be comprehensive enough to meet possible risks and regulations. Information security readiness means operational reliability for the company and properly done information security policies can be seen as a quality of the organization’s services. The policy should have clear instructions to employees how to follow safe information life cycle (Figure 4). For example what kind of data needs to be encrypted before it’s shared and what is the company’s procedure to destroy the sensitive material. The lack of security actives create additional work and possible extra costs for the business (SANS institute 2003)

Figure 4 Sensitive data lifecycle management

Critical information classification	
Finding The management doesn't have a clear picture of the existence of the company's security guidelines or its content. They don't understand all the regulation requirements what they need to follow. The company still haven't adopted any plans or processes to improve their information security considering the GDPR requirements.	
Conclusion The unsafe practices can cause business risks and extra costs for the business. Not having clear security policies which are followed by every employee can cause compliance problems towards GDPR. Without a clear methods the budgeting, resource planning and scheduling information security related developments can be slow and difficult to do.	
Recommendation	
Recommendation 1 Main stakeholders take information security into account and budget resources from the next fiscal year for being compliance to GDPR requirements.	1
Recommendation 2 The current level of the company's security policies is being evaluated. The instructions are divided to cover different roles inside of the organisation.	1
Recommendation 3 The employee instructions for handling confidential information are included into security policies. This instruction should include all the steps which are mentioned on (Figure 4): Sensitive data lifecycle management.	1

Table 2 Critical information classification

6.2 Information security service providers

The companies are not executing all their business processes by themselves, so it is important to find correct service suppliers. The service suppliers who can provide essentials services reliably and cost effectively. For small companies it is important to evaluate vendors and find the best suppliers to meet the business goals. The stability is one of the key drivers for this particular company. They customer register is updated every day from all around the country, so the platforms have to be as reliable as possible. The chosen service providers and vendors have to follow SLA (Service Level Agreement) strictly which has made with the company. Still it is the case companies' responsibility to evaluate the SLA is followed at the agreed level. It is clear this size of the company could not do their business without third part service providers, but there are large numbers of the service providers who are offering services to update customer register and help them with the financial management. Now when the case company's business is growing fast and expanding processes are running it is important to find the best vendors who can provide essential services and who are willing to develop their own internal processes to meet case companies' business goals and expanding processes. The vendors have to be evaluated even more carefully, if they have role on companies' risk management. In this case the case company works as a registrar who collects the information and the third part vendor works as information administrative who store the information into their servers (COBIT 5. 2014). The roles and responsibilities considering the GDPR requirements have to be agreed with the service providers on contract.

The SLA (Service Level Agreement) is essential contract for every company who are using third part service providers. The service buyer and service provider evaluate together specific service levels and metrics what have to be monitored by service provider. The purpose of the agreement is to define minimum performance levels. Define how to performance is monitored and what are the reporting methods. One of the pitfalls is use too simplistic performance indicators. For instance the service provider is sending an annual report of their performance levels and it might show the servers have been running 97% of their time and they have reached the requirements of SLA. This kind of report would be too vague. 3% when the servers have been down might mean a continuous period of four days and this kind of downtime has crucial effect on small companies' business. This is one of the reasons why the possible penalties or sanctions have to be written down on SLA contract. However the SLA contract has to be done without unrealistic expectations of service levels and this why the service buyer should always be able to provide essential documents to co-operating partners. For example the strategy and possible expand processes, information and physical security policies and list of regulation which are linked to companies' business industry (COBIT 5. 2014).

SSL (Secure Sockets Layer) is an effective protocol to secure companies' fluent telecommunication. Especially for companies who has booking system in their website or they transfer sensitive information of their customers. Even now the largest internet browsers like Google Chrome and Mozilla Firefox alert people who are accessing website without SSL certification not to add any personal data or payment card information into these websites (Figure 5). These kinds of warnings might have an impact for companies' business and potential new customers (Varmenne ja luottamuspalvelut. 2017)

This how the website domains appears to users after new SSL certification change (Figure 5). I did the benchmark to the case companies' business competitors and all of them were ready for new SSL requirements. The SSL certification is not answer of all problems and some professionals have wondered why the browser warns so aggressively about websites without certification. But still it is only natural the customer who doesn't know the SSL requirement choose the secured website instead of unsecured website which has a red warning on it. (Varmenne ja luottamuspalvelut. 2017).

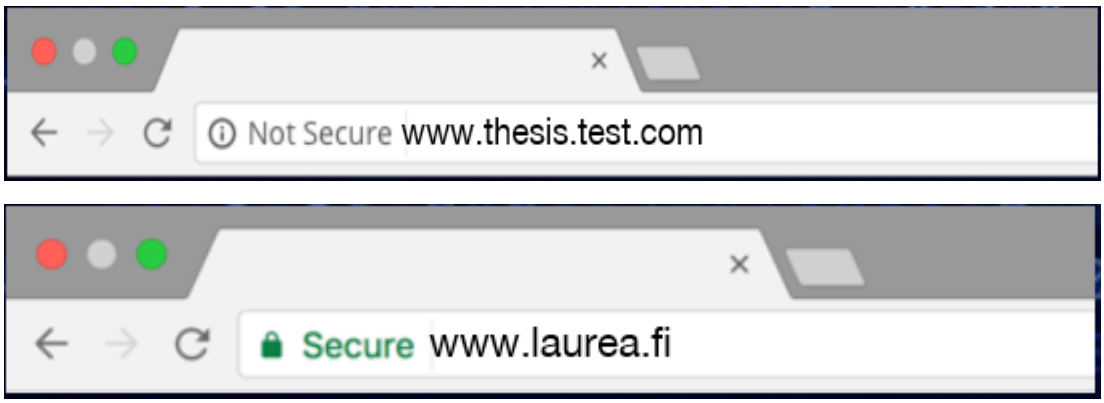


Figure 5 SSL certification on web browser

The certification assessment can be made through SSL certification websites for free. But this means the company itself or someone who is managing the website has to have enough of skills to encrypt the current website. The certification itself is inexpensive even bought from third party vendors. The prices are approximately 80€ per year. The certification can be bought from small vendors or large telecommunication companies. The company could publish with their vendors a data privacy policy as security and marketing tool on their website for their customer and business partners. The data privacy policy would give clear answers what information is collected, why it collected and where it is saved.

Information security service providers	
Finding The company doesn't have written service level agreements with the service providers. They don't know their responsibilities as data collector. The accurate requirements for vendors who works as a data administrative is not set.	
Conclusion This might lead into situation where company is not compliance with the regulation. Without proper contract handling there might be additional work costs and expenses for the company.	
Recommendation	
Recommendation 1 Company will publish a data privacy policy on their website	**3**
Recommendation 2 The company buy SSL certification from the service provider who has access to their server.	**2**
Recommendation 3 The company verify that all of their service providers are compliance towards GDPR and requires accurate service level agreements	**1**

Table 3 Information security implementation

6.3 Roles and responsibilities

To get the best capacity of companies' processes from business and security point of view is good to concentrate on roles and responsibilities. All the employees should know their role and responsibilities inside of the company. The company's employees should work toward same business goals and this why the roles should be divided comprehensively. The top level of the organisation carries the biggest responsibility because they have to monitor and control the business and security processes. The clear security processes combined to business goals can save money and reduces employee's workload (Karee & Benzel. 2008)

The clear structures of roles and responsibilities inside of the organisation have extensive benefits. The information security should be developed inside of the company as a broad process where training needs and communication has taken into account. The responsibilities and reporting practices should be clearly defined to increase effectiveness of internal and external communication. The clear roles have an impact also for the GDPR, because the regulation requires companies to nominate persons from the organisation who takes responsibility of handling the data privacy for internal and external parties. Usually for smaller companies it's not always mandatory to nominate DPO. But if the company doesn't nominate the DPO from organisation they still have to register a registry administrator whose main responsibility is to control register and requirements of regulation (Jordan & Sowerby. 2016).

The RACI chart (responsible, accountable, consulted and informed) was used to identify what are the responsibilities of main stake holders. The organisation can use the same method of finding any internal or external responsibilities. These charts help them to monitor security resources regularly and find correct corresponds and back-up persons for each critical processes. The same method can be used to manage project duration and expenses. This is also an effective way to prevent individuals from getting too large admin rights. This is one way how the company force their employees to do cross checks for critical processes. For example the same person who enters the invoice into system can't approve it (Doglione. 2016).

At this moment the company has four main owners, but only one of them takes the responsibility of critical business management processes. This is a risk which should be mitigated for business continuity purposes.

Critical business processes	**Stake holder 1**	**Stake holder 2**	**Stake holder 3**	**Stake holder 4**
Financial management	R, A	I		
Infrastructure & registers	R, A			
Agreements	R, A	I		
Recruitments & Training	R, A	A, I		
Marketing and sales	R, A	R, A	R, I	R, I
Security processes	A	I	I	I

Table 4 RACI chart

From the RACI table and from the interview sessions it is easy to summarize the company doesn't have a back-up person for each critical business processes and the same persons can do actually same task twice (Table 4). The main stakeholder of the company (Stake holder 1) has too broad responsibilities compared to other main stake holders. This is not effective business continuity planning where company should always be able to restore their business operations in all situations. At this moment the company has not accepted any levels of performance in case of a disruption. For instance, if something would happen to "Stake holder 1" the organisation would face difficulties on running operational processes and this could result in service downtime. When the company decide to clear their roles and responsibilities it is good to concentrate also for the culture change. The culture change will be presented in chapter 6.4.

Roles and responsibilities	
Finding The management does not have a clear picture of the roles inside of the company. Now the CEO has too broad responsibilities comparing to other stakeholders in critical processes. The company has not authorized anyone to control security processes.	
Conclusion This might cause dangerous working combination inside of organisation. Without back-up persons to critical processes of the company can face service downtimes.	
Recommendation	
Recommendation 1 The company start planning business continuity plan and uses RACI matrix table to clear roles and responsibilities.	1
Recommendation 2 One of the main stakeholders takes responsibility to help employees with security related issues. He or she takes responsibility of security communication and methods.	2

Table 5 Roles and responsibilities

6.4 Security knowledge

The company should organize regular targeted training for all its employees. The training is planned on a risk based basis and it uses of practical examples which is related to healthcare business industry. In this case the company doesn't have their own security personnel, so the outsourced security professional could handle the actual training. Especially for smaller domestic companies it is usually easier to train their employees to control unwanted risks to happen that it is for massive global enterprises. Attacks and defence in technology has become more and more complex all the time. Complexity adds exposure for human errors, so the managers and employees should be familiar with the company's security instructions well enough to know how to act accordingly in different situations (Figure 6). Again the whole protocol starts from the top, so from those people who are responsible for running the business and determine the responsibilities. They have to choose the level of security knowledge what they are demanding from their employees (Security standard council. 2014)

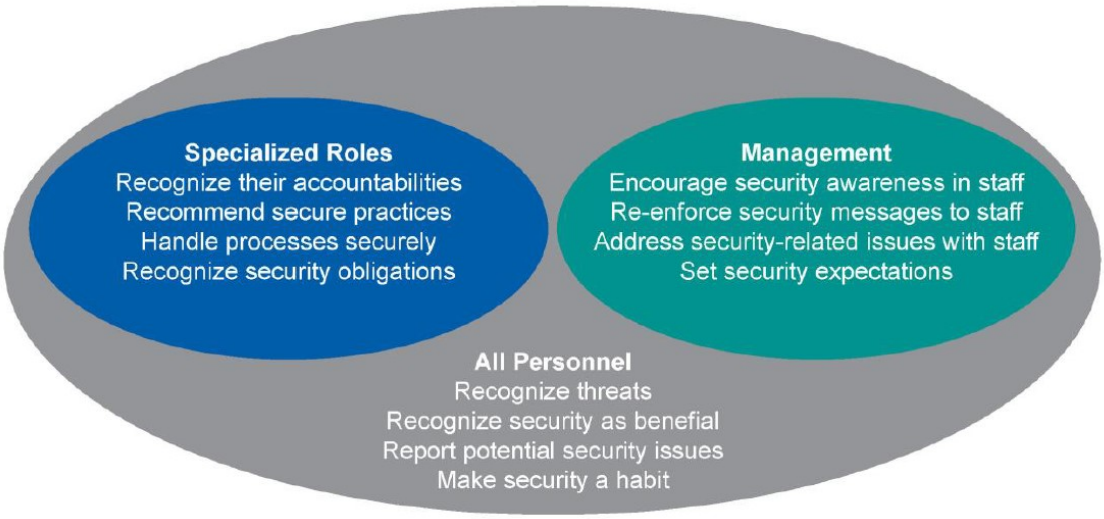


Figure 6 Security awareness roles for organisation

The case company has a very good training program for their employees to do their actual work. But they don't organize any training considering the physical or information security. For example training about security classification and social engineering would create a totally different culture inside of the organisation. In my opinion it would be very important the employees would have the basic knowledge of information security. Right now the company has less than a year make and implement a data protection improvement program. With this program the employees should gain knowledge and methods to prevent crimes and data breaches to happen. The GDPR requires companies to inform all data breaches in 72 hours to supervisory authorities. In 72 hours the company should be aware why this was happen and what was stolen. After this the authorities evaluate was everything protected according the regulation. The company needs to notify data subjects without any delay. Everything has to be done rapidly, so creating the process for notifying the authorities can be a lifesaver for company (Jordan & Sowerby. 2016).

The culture change in this size of organisation is easy to do, but it has to be done before it's too late. With this report I believe the case company understand the importance of information security and their own shortcomings or at least weaknesses for upcoming regulation. The customers can directly make formal complaints to GDPR supervisor authorities, if they feel their privacy rights have been violated. One of the first things what supervisor authorities are going check is how the employees are educated to understand regulation standards (Boardman, R. 2017)

ADKAR (Awareness, Desire, Knowledge, Ability, and Reinforcement) method by Prosci Inc is an effective method to implement new processes (Figure 7). The awareness is initiation step for a company who understand the shortcomings and wants to do something about it. In this step for a smaller company it is good to have business approach and identify targeted business outcomes from the project. It is important the key stake holders take part for the change and they raise awareness among the employees. The main stake holders should always be the project owners, because their participation in a project brings added value among employees (Hiatt. 2017).

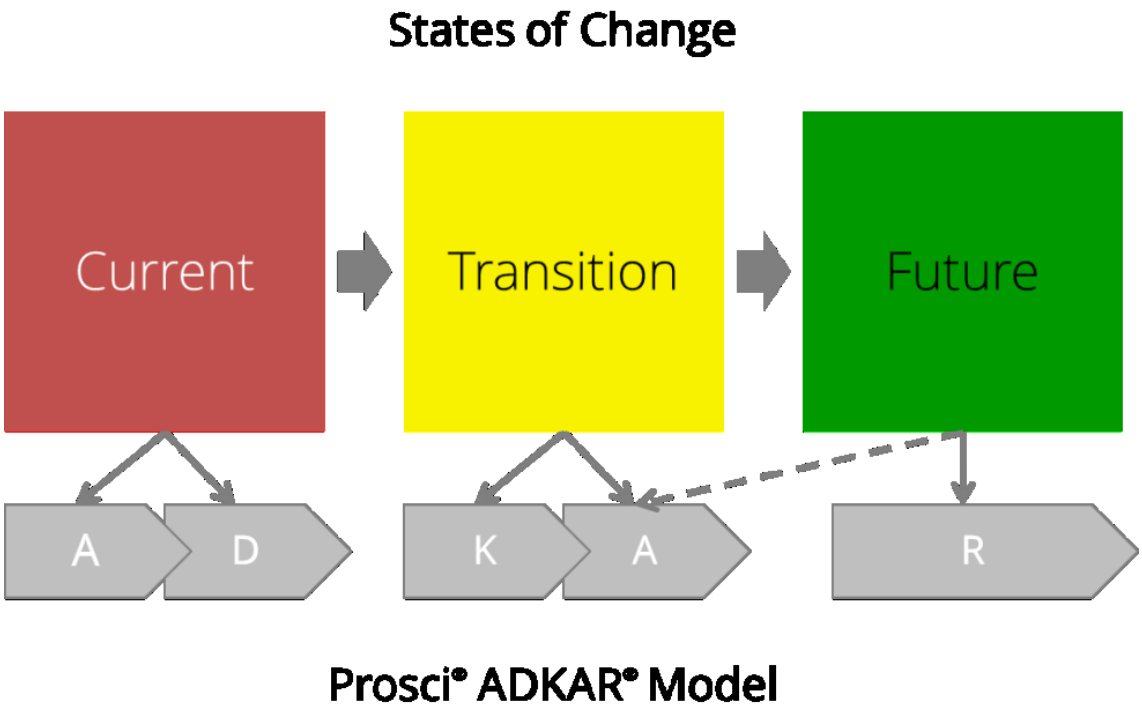


Figure 7 ADKAR states of change

The desire is the step after awareness where the methods are defined. All the employees should be given an explanation why the change is needed, what are the goals for the project. The actual vision implement starts in this phase. It is good to find the best dialogue channels to share information, but in this size of the company the inner meetings are the most effective way to share information among everyone. It is good to foster internal communication channels for sharing the knowledge inside of organisation (Hiatt. 2017).

After the first phases it's good to start evaluating current knowledge and methods to make culture change as effective as possible. All the relevant and committed people for the project should have recognized already in these phases. In steps knowledge and ability it's good to benchmark benefits from different activities and gather best practices in result of understand what can be learn from the past activities and build mutual operating procedures for the future. The reinforcement is phase where the change should be sustained. The changes what have been done during the process should be implemented into companies' critical processes. The recognition should be visible by main stakeholders to maintain the commitment of all employees (Hiatt. 2017).

Security knowledge	
Finding The company doesn't have any training considering the information security. This might lead into situation where the employee doesn't know how to act in different situations. The security risks are not measured or known by employees.	
Conclusion The users may cause avoidable security risks.	
Recommendation	
Recommendation 1 Create a targeted training plan for all employees. The training is planned on a risk based basis and it uses of practical examples which is related to healthcare business industry.	**1**
Recommendation 2 The company implement the culture change which is based on security basis. The training and culture change cover physical and electronic security.	**2**

Table 6 Security knowledge

6.5 Handling the confidential information

For the evaluating basic principles of information security I chose to use the CIA (Confidentiality, Integrity and Availability) model (Figure 8). The method is widely used and it provides three crucial sections which are closely linked to information security and data classification. With this research method I try to emphasize the critical assets what the company needs to protect. I will evaluate the main stake holders' level of information security knowledge and are they providing all the essential tools that their employees can do their work safely.

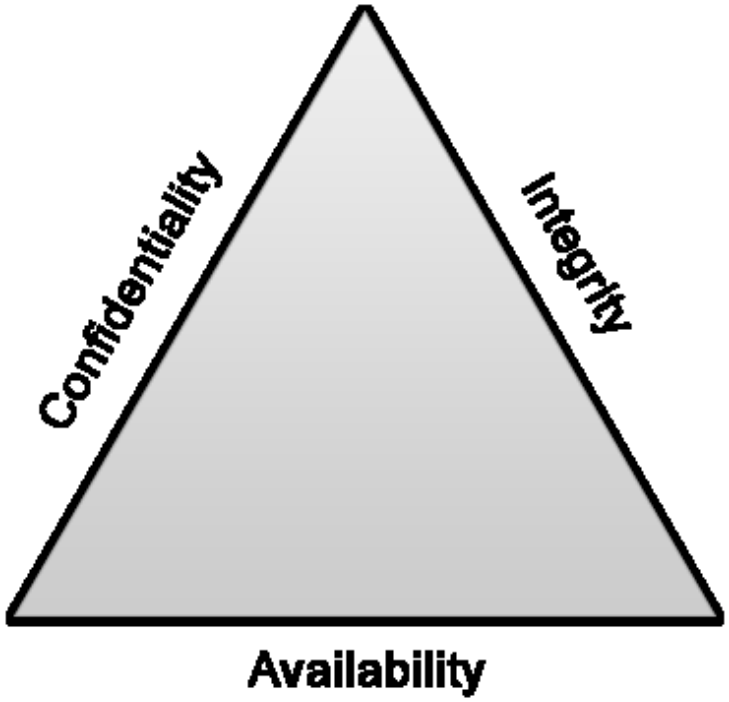


Figure 8 CIA method

Herberger (2012) Confidentiality is an important piece of each company's information security. From these sections is the most linked to the privacy. Its primary purpose is to enable the necessary data are only available to persons who need it. This is one of the key factors about General Data Protection Regulation as well because the person who has given their consent to save their information into systems has the right to cancel their consent whenever they want (the right the be forgotten). This also mean the person has right to see the list of all people who has handled or seen their information. This is major change for all companies, because the case company needs to request permission from all of their customers to save any information considering them. The companies can't use pre-ticked boxes anymore to request consent and the permission have to be asked clearly and intelligibly (Boardman, R. 2017).

Herberger (2012) Integrity means when the information is shared, it will remain unchanged through its whole life cycle, so basically the information remains exactly the same from send-

er to receiver. This is one of the key aspects for companies whose focus is to expand rapidly their business processes in the near future. The privacy by design is one main thing what the companies needs to take into consideration before they implement new projects. Privacy by design means the company have necessary evidences and they can assign they have took privacy and data protection into consideration in their processes. If the company implement new services or expand their business they need to have but now it's time to act and implement the necessary changes to be compliance considering the regulation (Boardman, R. 2017).

Herberger (2012) the purpose of availability is to ensure that information is available whenever it is needed. This can be linked to accountability which is also a new update in GDPR. Accountability is an indication of the obligation the company itself have updated documentation what information is saved from the customers. What are the reasons why the information is saved and where is it used? And finally who has to access into information. The company should have necessary opportunities to present only those employees have an access to see customer data that need it for their work (Boardman, R. 2017).

Handling the confidential information	
Finding In some cases the confidential information is sent unprotected to the recipient. The company doesn't have clear instructions how to share information for internal and external parties.	
Conclusion This might cause business risks which are preventable.	
Recommendation	
Recommendation 1 The management ensures there is instructions for all employees how to share information. And what are the correct tools to do it. The risk management evaluation is made for all the systems.	1
Recommendation 2 The company launch data protection development project. This maps the company's data protection requirements and assesses the current level of data protection and the necessary measures to reach the target compliance.	1

Table 7 Handling of confidential information

7 Methodology

The research projects can be done with different methods. Before starting this project I compared empirical and theoretical research methods and this how tried to find the most suitable research method for this particular project. The research methods can be changed during the project. But usually the research projects have limited economic resources and time limits, so it's good to make limitations from all available methods and choose one research method to cover the first phases (Koppa).

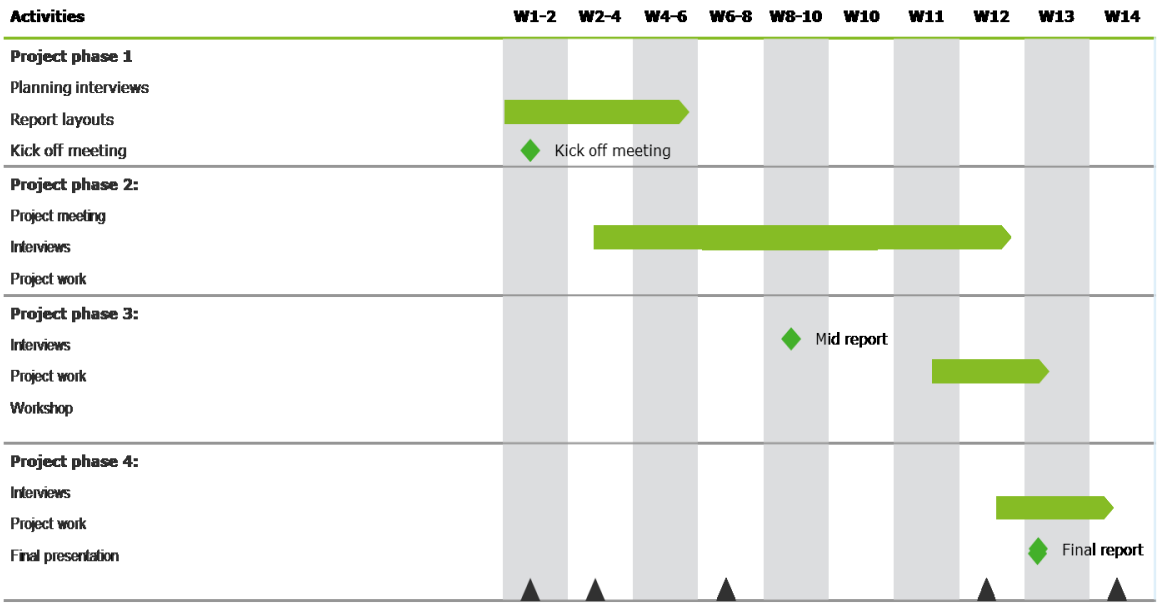
The theoretical research method can be based on existing documentation and it could have been used in this project. However the case company didn't have existing documentation considering their current information security readiness, so I decided to use empirical research methods. This method is more suitable for this specific purpose where the current state is compared the upcoming regulation. With this method the object was to use open ended questions, where I used the question frame from ISO 27001 without showing the questions before hand. Interviews were held to main stake holders of the company. If there would have been clear contradictions between the answers and my own observation I would have been comparing answers between employers and employees. But the main stakeholder was very open and interested about the project, so he provided truthful and clear answers to all my questions. If I would have done more interviews, I would have wanted to do interviews anonymously. This enables the respondents reply as faithfully as possible with own opinions. This is one the key things when thinking how to do an ethical survey where respondents don't have to fear being punished for giving their own opinions. With these answers I analysed my findings and compared them to regulation guidelines (Kustula 2015). The open ended questions can be found from appendix chapter (appendix 1).

The quantitative is effective research method, if we would like to compare the company's business methods to another company or if I would have done this same project for a large enterprise which has many employees. I would have chosen this method, if I would have been comparing or done benchmark data analysis. The quantitative method is also an effective way to analyse results from opinion pool where to data has been collected from many respondents. This is an effective research method for example at surveys where the average data is tried to achieve (Kustula 2015).

The qualitative research method was more suitable to this specific purpose because the idea is to measure quality of existing methods and what can be improved. Because of the upcoming regulation and frameworks I had a theoretical background to back up my questions. For both ISO standards and GDPR gives a reader guidelines how the things should be, but they are not clearly give you answer how to do it. This why I wanted to have face to face meetings with the main stakeholder and together evaluate which recommendations can be implement-

ed at first. This was also a good research method because there are clearly only few people in this organisation who can answer to questions considering the management. The idea is to give an explanation to case company why the changes have to be done before 2018 when the GDPR comes into effect (Kustula 2015).

Before I started to do this project I made a project schedule for case company. Together with the company we decided to follow this plan (Table 8). The final report will be given to the contact persons as soon as possible.



Activity duration

Milestones

Interviews & status meetings

Table 8 Project schedule

8 Research results

Like it was mentioned in chapter 7 the method what I used in this project was qualitative research method. First, my purpose was to compare the existing security documents with the new data protection legislation, this how I would have done so-called theoretical desk assessment for the company (Koppa). However the case company didn't have existing politics except the compulsory registry documents, so this why I ended up doing an empirical study of the comparison of interview results to the theoretical reference frames. The open ended questions were the right decision in my opinion, because the frameworks what I used to build my questions gives mainly the target states how the things should be. But not necessary advice or give tools to reach these target states.

My research methods and results were largely based on opinions, so I can't claim the results are the most reliable. But the project scope was to give guidelines and get an insight into the adequacy of processes. The analytical result comparison is hard to do in this project, but it's common for projects like this. In quantitative research it's more important than it is in qualitative projects the results are justified and the same results can be obtained with different ways (Koppa). In this project I could have used more theories to analyse the answers and backup my findings. Now, I have only used the ISACA and ISO 27001 frameworks in the most of the parts. One my main targets were that the same research methods what I choose could be used in any same sized organisation when implementing the GDPR readiness assessment.

I'm very pleased to see the management has already done some changes for the recommendations which were given in chapter 6 during this project. The company has bought correct certifications to protect their website and they have a new customer database where one of the largest telecom operator in Finland works as their data administrator. All the technical developments have been documented into excel file, so the documentation can be presented to the supervisory authorities. This is an extremely good start to fulfil an indication of the obligation. At this moment the company negotiate with telecom operator of possible ways how to make restricted spaces only for those who need to use individual customer data. The employee register has been moved to a separate platform and the register administrative has been nominated from the company or at least now his role is clear for all the employees.

The principles of information lifecycle have been brought into the company's processes already (Figure 4). The new platform enable company to store and share information with ways what GDPR requires. The company is currently looking for a service provider who has certified methods to destroy physical sensitive information, so it won't end up with the wrong hands. At first one security information bin will be placed in the largest clinic where the physical information including papers, CDs, USB-sticks etc. will be destroyed.

I believe the management sees security now as beneficial tool and the new culture change inside of the organisation develop the ways of how the things are done. After some time the new ways to do things are just the normal ways to act, this how the culture change inside of the organisation starts to get in touch with all the employees. The main stake holder has already got meetings considering the roles and responsibilities (Table 4). All these development and instructions will be written down and this how the company will get preliminary security policies.

The company has made preliminary training materials for new employees. The short introduction is presented when the employee arrives to write employment contract or during the first days. Later this year I have promised to help company to make better training material for all of their current employees. The both information and physical security will be taken into account as part of the training days. This how the management will encourage following security awareness plans and setting the level of security knowledge what they are expecting from their employees (Figure 6).

9 Conclusion

This was interesting project to do because I haven't done this kind of assessment before, so this was extremely educational for me. I'm interested about data protection and privacy, but I didn't realize how much work it takes to understand even the basic principles of different privacy regulation. I'm extremely satisfied that I got such a good case company for this project. They were always available when I needed them and they were highly motivated into this project. Still I'm very happy that I chose this specific subject for my thesis, because there will be lots of companies who needs help to evaluate their information and data privacy matters, so I believe I would be more ready to take part of this projects in the future as well.

I believe the case company has at least better understanding what they should do before 25th of May.

- Now the company should be able to identify what is sensitive data for them?
- What are the locations and accessibility levels to handle the critical information?
- How to classify the data which has value to the organisation?

I suggest the company contact GDPR supervisory authorities for the final steps, which are linked to the monitoring security practices what they have implemented (Figure 3). Together with the company's CEO we agreed that I'll try to help them in the future as well, with the training materials and in other tasks where I'm able to help them. I personally see this as a create way of learning more about information security and project management.

I didn’t do the middle report for company even thought it was planned in a kick-off meeting. We had so many face to face meetings and phone conversations with the CEO, so there was no point of doing it. The actual project scope was really hard to follow. Maybe because I don’t have previous experience of doing large audit related projects like this. There were few changes what I had to do compare to first project plan. But it’s normal in these projects. It’s hard to choose only one method what will be followed during the whole project. Still I should have chosen the methods more carefully, because chancing the methods during the project consumes the project time and resources. So there are still lots of space for improvements, but altogether I am satisfied with the result of the work. One of the most difficult things was to compare the actual standard to the company who doesn’t have the biggest resources to use towards business security. In the end we got good results with the company. And like it said in the introduction the security can’t be done once and leave it there. The process has to be continuous and I feel the case company is on the right tracks.

9.1 References

Anatomy of a data breach. Accessed 21.2.2017. http://about-threats.trendmicro.com/RelatedThreats.aspx?language=cn&name=Anatomy%20of%20a%20Data%20Breach

Baiati, N. 2017. How does GDPR impact the healthcare sector. Accessed 29.5.2017. http://adigaskell.org/2017/02/04/how-does-gdpr-impact-the-healthcare-sector/

Boardman, R. 2017. Guide to the General Data Protection Regulation. Accessed 14.1.2017. https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

Chambers, J. 2014. What does the Internet of everything mean for security. Accessed 4.3.2017. https://www.weforum.org/agenda/2015/01/companies-fighting-cyber-crime/

Church, P. 2016. The General Data Protection Regulation. Accessed 15.1.2017. http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf

COBIT. 2014. Vendor management. ISACA

Cost of data breach study. 2016. Accessed 20.4.2016 https://app.clickdimensions.com/blob/softchoicecom-anjf0/files/ponemon.pdf

Clarke, R. 1997. Situational crime prevention. Accessed 18.5.2017. http://garnerclancey.com/pdfs/Crime%20Prevention%20Situational.pdf

Doglione, C. 2016. Understanding responsibility assignment matrix. Accessed 18.1.2017. https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

European council. 2016. Official Journal of the European Union. Accessed 29.5.2017. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

EU yleinen tietosuoja-asetus. 2016. Accessed 2.3.2017. http://www.privacy-regulation.eu/fi/

Everest, D. 2018. Accessed 5.2.2017. http://theiia.org/bookstore/downloads/freetomembers/0_1045.dl_gtag10.pdf

Filkins, B. 2016. IT Security spending trends. Accessed 1.3.2017
https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

Gil, P. 2017. What are black hat and white hat hackers. Accessed 27.4.2017.
https://www.lifewire.com/black-hat-hacker-a-white-hat-hacker-4061415

Herberger, C. 2012. Information availability is foundational. Accessed 3.3.
https://blog.radware.com/security/2012/02/in-security-information-availability-is-foundational/

Hiatt, J. 2017. What is ADKAR model. Accessed 1.2.2017.
https://www.prosci.com/adkar/adkar-model

Jordan, A & Sowerby, M. 2016. Preparing for the general data protection regulation. Accessed 8.2.2017 https://www.securityforum.org/uploads/2017/03/ISF_Preparing-for-the-General-Data-Protection-Regulation_Digest.pdf

Karee, L & Benzel, T. 2008. An introduction to the business model for information security. Accessed 6.4.2016.
http://www.isaca.org/KnowledgeCenter/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf

Koppa. Jyväskylän Yliopiston. Menetelmä polkuja humanisteille. Accessed 10.5.2017.
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku

Krazit, T. 2016. Employees Are the Weakest Link in Computer Security. Accessed 3.2.2017
http://fortune.com/2016/06/20/employees-computer-security/

Kustula, S. 2015. Laadullinen ja määrällinen tutkimus opinnäytetyössä. Accessed 30.4.2017
http://esseepankki.proakatemia.fi/laadullinen-ja-maarallinen-tutkimus-opinnaytetyossa/

Limnéll, J & Majweski, K. 2014. Kyberturvallisuus. Docendo

Opi tietosuojaa. 2017. Accessed 4.6.2017.
https://opitietosuojaa.fi/index.php/fi/aloitus/tietosuoja

Rodgers, S. 2012. Data classification. Accessed 15.3.2017.
https://www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security

SANS institute. 2003. The security lifecycle. Accessed 4.1.2017
https://www.giac.org/paper/gsec/3018/security-lifecycle/105040

Schmittling, R. 2010. Performing a security risk assessment. Accessed 3.5.2017.
https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx

Security standard council. 2014. Best practices for implementing a security awareness program. Accessed 3.4.2017.
https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Situational crime prevention. Accessed 2.3.2017.
http://criminology.wikia.com/wiki/Situational_Crime_Prevention

Varmenne ja luottamuspalvelut. 2017. Accessed 3.1.2017
https://www.telia.fi/yrityksille/tuotteet/tietoliikenne/varmenne-ja-luottamuspalvelut/ssl-palvelinvarmenne

Figures

Tables

Appendices

Appendix 1: Open questions for main stake holders

1. Onko johto hyväksynyt tietoturvapolitiikan?

2. Käsitelläänkö tietoturva-asioita säännöllisesti?

3. Oletko perehtynyt tietoturvaohjeistuksiin ja kuinka hyvin tunnet niitä?

4. Kenen vastuulla on raportoida viranomaisille väärinkäytöksistä?

5. Miten tietoturvavastuut on määritetty ja jaettu?

6. Miten tietoturva on organisoitu?

7. Miten tiedon omistajuus on määritelty/ onko kaikelle tiedolle määritelty omistajuutta?

8. Onko tiedon/laitteiden/ tietoverkkojen/ järjestelmien sallitut käyttötavat määritelty?

9. Luokitellaanko tietoa (esim. kriittisyyden mukaan)?

10. Onko tiedotettu ja opastettu mihin ja millä tavalla turvallisuuspoikkeamista ilmoitetaan?

11. Miten on ohjeistettu miten tietoa saa välittää ulkopuoliselle taholle?

12. Missä järjestelmässä ja millä tavalla tallennetaan työssä tarvittavaa luottamuksellista aineistoa?

13. Millä tavoilla välität luottamuksellista tietoa yrityksen sisäpuolella?

14. Millä tavoilla välität luottamuksellista tietoa yrityksen ulkopuolelle?

15. Onko käytössä pilvipalveluita, joihin tallennetaan luottamuksellista tietoa?

16. Mitä kriittisiä liiketoimintajärjestelmiä käytetään mobililaitteilla?

17. Missä säilytät tärkeää fyysistä aineistoa?

18. Miten tuhoat tärkeän fyysisen aineiston?

19. Miten toimit/ varmistaudut viestin lähettäjän tai soittajan oikeellisuudesta?

20. Miten jatkuvaa riskientunnistusta ja arviointia tehdään?

21. Onko prosesseja olemassa millä tietoturvariskejä arvioidaan?

22. Onko tunnistettu ja dokumentoitu yrityksen kriittiset tiedot ja prosessit?

23. Miten tiedonsuojaus on teknillisesti toteutettu?

24. Onko lokienhallintapolitiikka olemassa?

25. Millainen toimintatapa on luotu tietoturvapoikkeamien hallintaan?

26. Onko tietoturvaohjeistuksessa huomioitu eri työroolit?